(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-72717
(P2004-72717A)
(43)公開日　平成16年3月4日(2004.3.4)

(51)Int.Cl.[7]		F I			テーマコード（参考）
H04L	9/08	H04L	9/00	601F	5J104
H04L	9/32	H04L	9/00	675D	

審査請求 未請求　請求項の数 23　OL　（全 22 頁）

(21)出願番号　特願2003-128549(P2003-128549)
(22)出願日　平成15年5月7日(2003.5.7)
(31)優先権主張番号　特願2002-170798(P2002-170798)
(32)優先日　平成14年6月12日(2002.6.12)
(33)優先権主張国　日本国(JP)

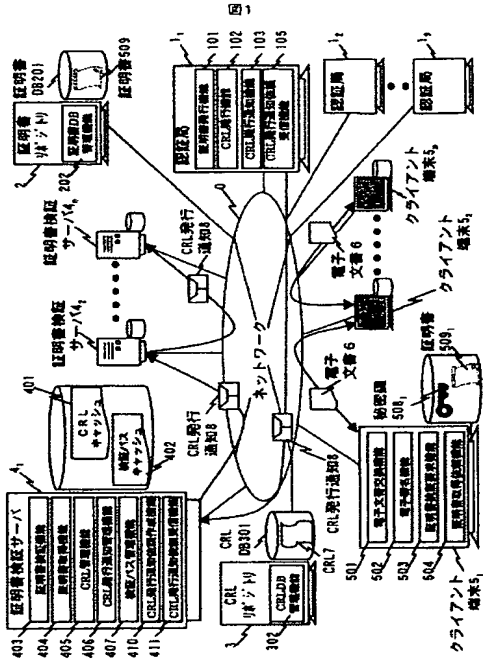
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(74)代理人　100075096
弁理士　作田　康夫
(72)発明者　鍛　忠司
神奈川県川崎市麻生区王禅寺１０９９番地
株式会社日立製作所システム開発研究所内
(72)発明者　藤城　孝宏
神奈川県川崎市麻生区王禅寺１０９９番地
株式会社日立製作所システム開発研究所内

最終頁に続く

(54)【発明の名称】ＣＲＬ発行通知機能付き認証基盤システム

(57)【要約】
【課題】証明書の有効性判定処理を高速化するためにＣＲＬをキャッシュすると、認証局がＣＲＬを緊急に発行した場合に、キャッシュしている前記ＣＲＬが最新のものではないため、証明書の有効性検証結果の精度が保証できない。
【解決手段】前記ＣＲＬが発行された場合に、前記認証局から前記証明書検証サーバにＣＲＬ発行通知が行われ、かつ、当該ＣＲＬ発行通知を受信した前記証明書検証サーバは最新の前記ＣＲＬをキャッシュするため、証明書有効性検証結果の精度が保証できる。

図1



1

【特許請求の範囲】
【請求項１】
証明書を発行する証明書発行手段と、ＣＲＬを発行するＣＲＬ発行手段とを備えた認証局と、
前記認証局が発行した前記ＣＲＬを格納するＣＲＬ格納手段を備えたＣＲＬリポジトリと、
前記証明書の有効性を検証する証明書有効性検証手段と、前記ＣＲＬリポジトリから取得した前記ＣＲＬをキャッシュするＣＲＬキャッシュ手段とを備えた証明書検証サーバと、を備え、
前記認証局は、前記ＣＲＬを発行した場合に「ＣＲＬが発行された」旨を通知するＣＲＬ発行通知を、前記証明書検証サーバに送信するＣＲＬ発行通知送信手段を備え、
前記証明書検証サーバは、前記認証局から前記ＣＲＬ発行通知を受信するＣＲＬ発行通知受信手段を備える
ことを特徴とする、認証基盤システム。
【請求項２】
請求項１記載の認証基盤システムであって、
前記証明書検証サーバの前記ＣＲＬキャッシュ手段は、前記ＣＲＬ発行通知受信手段によって前記ＣＲＬ発行通知を受信した場合に、前記認証局が新たに発行した前記ＣＲＬを前記ＣＲＬリポジトリから取得する
ことを特徴とする認証基盤システム。
【請求項３】
請求項１または２記載の認証基盤システムであって、
前記証明書検証サーバは、前記ＣＲＬが新たに発行されたことを発見した場合に、予め登録された他の証明書検証サーバに対して、「ＣＲＬが発行された」旨を通知する、ＣＲＬ発行通知送信手段を備える
ことを特徴とする、認証基盤システム。
【請求項４】
証明書の有効性を検証する証明書有効性検証手段と、当該証明書有効性検証手段が前記証明書の有効性を検証するために構築した検証パスをキャッシュする検証パスキャッシュ手段とを備えた証明書検証サーバと、
電子署名を検証する電子署名検証手段と、前記証明書検証サーバに前記証明書の有効性検証を依頼する証明書有効性検証依頼手段を備えたクライアントと、を備え、
前記証明書検証サーバは、前記検証パスを構築した場合に、予め登録された他の証明書検証サーバに当該検証パスを送信する検証パス送信手段を備え、
前記検証パスキャッシュ手段は、他の証明書検証サーバから前記検証パスを受信した場合に、当該検証パスをキャッシュする
ことを特徴とする認証基盤システム。
【請求項５】
証明書を発行する証明書発行手段を備えた認証局と、
前記認証局が発行した前記証明書を格納する証明書格納手段を備えた証明書リポジトリと、

2

前記証明書の有効性を検証する証明書有効性検証手段を備えた証明書検証サーバと、
電子署名を検証する電子署名検証手段と、前記証明書検証サーバに前記証明書の有効性検証を依頼する証明書有効性検証依頼手段を備えたクライアントと、を備え、
前記クライアントは、前記電子署名を検証するために必要な前記証明書の取得を、前記証明書検証サーバに依頼する証明書取得依頼手段を備え、
前記証明書検証サーバは、前記クライアントから取得を要求された前記証明書を前記証明書リポジトリから取得し、かつ、前記証明書検証手段によって、当該証明書が有効であると判定された場合に、前記クライアントに当該証明書を送信する証明書取得手段を備える
ことを特徴とする認証基盤システム。
【請求項６】
証明書を発行する証明書発行手段と、ＣＲＬを発行するＣＲＬ発行手段とを備え、
前記ＣＲＬを発行すると同時に、前記証明書検証サーバに「ＣＲＬが発行された」旨を通知するＣＲＬ発行通知を送信するＣＲＬ発行通知送信手段を備える
ことを特徴とする認証局。
【請求項７】
証明書の有効性を検証する証明書有効性検証手段と、ＣＲＬをキャッシュするＣＲＬキャッシュ手段とを備え、
ＣＲＬが発行されたことを通知するＣＲＬ発行通知を受信するＣＲＬ発行通知受信手段、を備えることを特徴とする、証明書検証サーバ。
【請求項８】
請求項７記載の証明書検証サーバであって、
前記証明書検証サーバの前記ＣＲＬキャッシュ手段は、前記ＣＲＬ発行通知受信手段によって、前記ＣＲＬ発行通知を受信した場合に、新たに発行した前記ＣＲＬを取得する
ことを特徴とする証明書検証サーバ。
【請求項９】
請求項７または８記載の証明書検証サーバであって、
前記ＣＲＬが新たに発行されたことを発見した場合に、予め登録された他の証明書検証サーバに対して、「ＣＲＬが発行された」旨を通知するＣＲＬ発行通知送信手段を備える
ことを特徴とする証明書検証サーバ。
【請求項１０】
証明書の有効性を検証する証明書有効性検証手段と、当該証明書有効性検証手段が前記証明書の有効性を検証するために構築した検証パスをキャッシュする検証パスキャッシュ手段とを備え、
前記検証パスを構築した場合に、予め登録された他の証明書検証サーバに当該検証パスを送信する検証パス送信手段を備え、
前記検証パスキャッシュ手段は、他の証明書検証サーバ

から前記検証パスを受信した場合に、当該検証パスをキャッシュする
ことを特徴とする証明書検証サーバ。
【請求項１１】
電子署名を検証する電子署名検証手段と、証明書検証サーバに前記証明書の有効性検証を依頼する証明書有効性検証依頼手段を備え、
前記電子署名を検証するために必要な前記証明書の取得を、前記証明書検証サーバに依頼する証明書取得依頼手段を備える
ことを特徴とするクライアント装置。
【請求項１２】
前記証明書の有効性を検証する証明書有効性検証手段を備え、
取得を要求された前記証明書を前記証明書リポジトリから取得し、かつ、前記証明書検証手段によって当該証明書が有効であると判定された場合に、当該証明書を返信する証明書取得手段を備える
ことを特徴とする証明書検証サーバ。
【請求項１３】
請求項１記載の認証基盤システムであって、
前記証明書検証サーバは、ＣＲＬ発行通知依頼メッセージを作成する、ＣＲＬ発行通知依頼作成手段を備え
前記認証局は、前記ＣＲＬ発行通知依頼メッセージを受信する、ＣＲＬ発行通知依頼受信手段を備え、
前記認証局の前記ＣＲＬ発行通知送信手段は、当該認証局に対して前記ＣＲＬ発行通知依頼メッセージを送信してきた証明書検証サーバに対して、前記ＣＲＬ発行通知を送信する。
【請求項１４】
請求項１３記載の認証基盤システムであって、
前記証明書検証サーバは、
他の証明書検証サーバから前記ＣＲＬ発行通知依頼メッセージを受信する、ＣＲＬ発行通知依頼受信手段と、
前記ＣＲＬ発行通知を受信した場合に、前記ＣＲＬ発行通知依頼メッセージを送信してきた証明書検証サーバに対して、前記ＣＲＬ発行通知を転送する、ＣＲＬ発行通知管理手段を備える。
【請求項１５】
請求項６記載の認証局であって、
ＣＲＬ発行通知依頼メッセージを受信する、ＣＲＬ発行通知依頼受信手段を備え、
前記ＣＲＬ発行通知送信手段は、前記ＣＲＬ発行通知を、受信した前記ＣＲＬ発行通知依頼メッセージの送信元に送信する。
【請求項１６】
請求項７記載の証明書検証サーバであって、
ＣＲＬ発行通知依頼メッセージを作成する、ＣＲＬ発行通知依頼作成手段を備える。
【請求項１７】

請求項１６記載の証明書検証サーバであって、
他の証明書検証サーバから前記ＣＲＬ発行通知依頼メッセージを受信する、ＣＲＬ発行通知依頼受信手段と、
前記ＣＲＬ発行通知を受信した場合に、前記ＣＲＬ発行通知依頼メッセージを送信してきた証明書検証サーバに対して、前記ＣＲＬ発行通知を転送する、ＣＲＬ発行通知管理手段を備える。
【請求項１８】
認証局が発行したＣＲＬを格納するＣＲＬ格納手段を備えたＣＲＬリポジトリであって、
前記ＣＲＬ格納手段が、新たなＣＲＬを格納すると、ＣＲＬ発行通知を送信するＣＲＬ発行通知送信手段を備える。
【請求項１９】
請求項１８記載のＣＲＬリポジトリであって、
ＣＲＬ発行通知依頼メッセージを受信する、ＣＲＬ発行通知依頼受信手段を備え、
前記ＣＲＬ発行通知送信手段は、前記ＣＲＬ発行通知を、受信した前記ＣＲＬ発行通知依頼メッセージの送信元に送信する。
【請求項２０】
計算機に、ＣＲＬの発行を監視し、新たなＣＲＬが発行された場合に、ＣＲＬ発行通知を送信するＣＲＬ発行通知送信手段を実現する、ＣＲＬ発行確認ソフトウェアであって、
ＣＲＬ発行通知依頼メッセージを受信する、ＣＲＬ発行通知依頼受信手段を実現し、
前記ＣＲＬ発行通知送信手段は、前記ＣＲＬ発行通知を、受信した前記ＣＲＬ発行通知依頼メッセージの送信元に送信する。
【請求項２１】
「ＣＲＬが発行された」旨を通知する、ＣＲＬ発行通知用データフォーマットであって、
新たに発行されたＣＲＬ自身を記載する項目を含む。
【請求項２２】
「ＣＲＬが発行された」旨を通知する、ＣＲＬ発行通知用データフォーマットであって、
当該発行通知より前に発行されたＣＲＬと、新たに発行されたＣＲＬとの差分情報を記載する項目を含む。
【請求項２３】
「ＣＲＬが発行された」旨を通知する、ＣＲＬ発行通知用データフォーマットであって、
新たに失効された証明書の識別情報の一覧を記載する項目を含む。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、公開鍵証明書の失効リストを発行する認証局と、公開鍵証明書の有効性を検証する証明書検証サーバと、上記証明書検証サーバを利用するクライアントと、

5

からなる認証基盤システムに関する。

【０００２】

【従来の技術】

政府認証基盤（以下、ＧＰＫＩ、と記述する）をはじめとして、電子文書の作成者を明らかにし、かつ、当該電子文書が改ざんされていないことを保証するために、公開鍵認証基盤（Ｐｕｂｌｉｃ　Ｋｅｙ　Ｉｎｆｒａｓｔｒｕｃｔｕｒｅ、以下、ＰＫＩ、と記述する）を利用したシステムが普及してきている（例えば、非特許文献１参照）。ＰＫＩを利用したシステムでは、電子文書に対して、電子署名を行う者（以下、署名者、と記述する）のみが保有する、秘密鍵（Ｐｒｉｖａｔｅ　ｋｅｙ）と呼ばれる鍵によって電子署名が施される。電子署名が施された電子文書を受信した場合には、上記電子署名を検証することで、電子文書の作成者と、当該電子文書が改ざんされていないことと、を確認する。

【０００３】

高い信頼が要求される用途では、電子署名の検証を行うためには、上記署名者の公開鍵証明書（以下、証明書、と記述する）に含まれている、公開鍵と呼ばれる鍵によって、当該電子署名を検証するだけではなく、上記署名者の証明書が電子署名を検証する者（以下、検証者、と記述する）にとって有効な証明書であるか否か、を確認する必要がある。上記署名者の証明書が上記検証者にとって有効であるか否か、を検証するには、（１）認証パスの構築と、（２）認証パスの検証と、という、処理が必要である。

【０００４】

認証パスとは、上記検証者から上記署名者までの信頼の連鎖であり、証明書のチェーンとして表現される。特に、認証局同士がお互いに証明書を発行しあうような場合には、相互認証証明書という、特殊な証明書を発行する。認証局$１_{１}$から認証局$１_{９}$までの９個の認証局が図２に示したような相互認証の関係を持っている場合には、認証局$１_{２}$が発行した証明書を持つ検証者から認証局$１_{１}$が発行した証明書を持つ署名者までの認証パスは、一番目が相互認証証明書$９_{１８}$、二番目が相互認証証明書$９_{６８}$、三番目が相互認証証明書$９_{４６}$、四番目が相互認証証明書$９_{２４}$、最後が検証者の証明書、という順序の証明書チェーンとなる。このようにして構築された検証パスを検証する方法については、上記非特許文献１に詳細に記述されている。

【０００５】

また、上記ＧＰＫＩの仕様書には、証明書の有効性を検証するモデルとして、エンドエンティティモデルと、証明書検証サーバモデルが記載されている。（例えば、非特許文献２参照。）上記証明書検証サーバモデルは、証明書の有効性を検証するために、クライアントに代わってオンラインで証明書の有効性を確認する機能を提供する、証明書検証サーバを利用する。

6

【０００６】

上記証明書検証サーバモデルは、上記エンドエンティティモデルに比べて、次のような利点がある。まず、上記証明書検証サーバモデルでは、上記認証パスを構築する認証パス構築機能をクライアントに実装する必要がないため、クライアントの署名検証プログラムを小さくすることができる。また、クライアントは上記証明書検証サーバの判定結果を信頼するため、上記証明書検証サーバの設定を変更するだけで、システム構成の変化に柔軟に対応できる。上記非特許文献２によれば、証明書が失効されているか否かを判定するには、上記認証局が発行する証明書失効リスト（Ｃｅｒｔｉｆｉｃａｔｅ　Ｒｅｖｏｃａｔｉｏｎ　Ｌｉｓｔ、以下、ＣＲＬ、と記述する）やＯＣＳＰレスポンダが利用される。

【０００７】

検証を行う毎に上記認証局から上記ＣＲＬを取得するのは効率が悪いため、特許文献１では、上記証明書検証サーバが上記証明書や上記ＣＲＬや上記検証パスをキャッシュすることにより証明書の有効性判定処理を高速化する方式が開示されている。

【０００８】

ところで、電子署名を検証したり、検証パスを構築したりするためには、署名者の証明書を入手することが必要である。署名者の証明書を入手する方法は大きく二つに分類することができる。

【０００９】

一つは、署名者からは電子署名付き電子文書が送付されるのみであり、当該署名者の証明書は別途入手する、という方法である。例えば、電子署名付き電子文書とともに、当該電子署名を検証するための証明書が格納されている場所を示すＵＲＬを通知する方法などが該当する。この方法では、上記検証者は、上記証明書が格納された場所（以下、証明書リポジトリ、と記述する）などにアクセスし、当該証明書を入手する必要がある。もう一つは、署名者が、電子署名付き電子文書とともに、当該電子署名を検証するために利用する証明書を添付して送付する、という方法である。

【００１０】

【特許文献１】

特開２００２－７２８７６号公報

【非特許文献１】

ＩＴＵ、ＩＴＵ－Ｔ　Ｒｅｃｏｍｍｅｎｄａｔｉｏｎ　Ｘ．５０９　“Ｉｎｆｏｒｍａｔｉｏｎ　ｔｅｃｈｎｏｌｏｇｙ　－　Ｏｐｅｎ　ｓｙｓｔｅｍｓ　ｉｎｔｅｒｃｏｎｎｅｃｔｉｏｎ　－　Ｔｈｅ　Ｄｉｒｅｃｔｏｒｙ：　Ｐｕｂｌｉｃ－ｋｅｙ　ａｎｄ　ａｔｔｒｉｂｕｔｅ　ｃｅｒｔｉｆｉｃａｔｅ　ｆｒａｍｅｗｏｒｋｓ”、ＩＴＵ、２０００年３月、ｐ．７－５３

【非特許文献２】

「政府認証基盤（ＧＰＫＩ）　政府認証基盤相互運用性

7

仕様書」ｐ．１８－２０，２７－２９、［ｏｎｌｉｎｅ］、平成１３年４月２５日、基本問題専門部会了承、［２００３年３月１４日検索］、インターネット＜ＵＲＬ：ｈｔｔｐ：／／ｗｗｗ．ｓｏｕｍｕ．ｇｏ．ｊｐ／ｇｙｏｕｋａｎ／ｋａｎｒｉ／０１０５１４＿２．ｐｄｆ＞

【００１１】

【発明が解決しようとする課題】

証明書の有効性判定処理を高速化するために上記ＣＲＬをキャッシュすると、上記認証局が上記ＣＲＬを緊急に発行した場合に、キャッシュしている上記ＣＲＬが最新のものではなくなる。特許文献１にはこの点について言及していない。

【００１２】

上記の課題を解決する方法の一つとしては、上記ＣＲＬが緊急発行された場合にも有効性検証が正しく行われるために、上記証明書検証サーバが、上記ＣＲＬの格納場所（以下、ＣＲＬリポジトリと呼ぶ）に定期的にアクセスし、上記ＣＲＬが更新されていないかを確認する方法がある。上記方法は、さらに、上記証明書検証サーバ自身がネットワークを介して確認を行う方式と、上記ＣＲＬリポジトリにＣＲＬ発行確認ソフトウェアを導入して確認を行う方式と、の２種類がある。

【００１３】

上記ＣＲＬが更新されていないかを定期的に確認する方法を利用して、上記証明書の有効性検証結果の精度を高めるためには、上記確認の間隔をできる限り短くすることが必要である。しかし、上記証明書検証サーバ自身がネットワークを介して確認を行う方式では、上記確認の間隔を短くするとネットワークの負荷が大きくなる、という課題がある。

【００１４】

一方、上記ＣＲＬリポジトリに確認を行うためのＣＲＬ発行確認ソフトウェアを導入する方式の場合には、上記ＣＲＬリポジトリの運営者と上記証明書検証サーバの運営者とが異なると、上記ＣＲＬ発行確認ソフトウェアのインストールが許可されず、上記確認が行えない場合がある、という課題がある。

【００１５】

また、複数の上記証明書検証サーバが存在する環境では、すべての上記証明書検証サーバが上記ＣＲＬリポジトリに導入された上記ＣＲＬ発行確認ソフトウェアを利用しなければ、すべての上記証明書検証サーバが同じ精度で証明書有効性検証を行うことができないため、稼動している上記証明書検証サーバの数を増減させたい場合には、上記ＣＲＬ発行確認ソフトウェアの設定を変更する必要があるが、上記ＣＲＬリポジトリの運営者と上記証明書検証サーバの運営者とが異なると、上記証明書検証サーバの数を柔軟に変更することが困難である、という課題がある。

8

【００１６】

さらに、上記検証パスをキャッシュしているとしても、上記認証局によって古い相互認証証明書が破棄され、新しい相互認証証明書が発行されていた場合には、新しい相互認証証明書を含む検証パスを構築する必要がある。

【００１７】

また、複数の上記証明書検証サーバが存在する環境では、複数の上記証明書検証サーバが、同じ上記証明書の有効性を検証した場合でも、各々の上記証明書検証サーバが上記認証パスの構築や、上記ＣＲＬの取得などを行うため、特定の上記ＣＲＬリポジトリや上記証明書リポジトリにアクセスが集中したり、ネットワークの負荷が大きくなったりする可能性がある。特許文献１にはこれらについて言及していない。

【００１８】

また、上記証明書を別途入手する方法では、上記クライアントは、上記証明書検証サーバに上記証明書の有効性検証を依頼するため、まず、上記証明書リポジトリにアクセスして上記証明書を取得しなければならない、という課題がある。

【００１９】

従って、上記各課題を解決する新たな手法が求められている。

【００２０】

【課題を解決するための手段】

本発明は、上記証明書を発行する証明書発行手段と、上記ＣＲＬを発行するＣＲＬ発行手段と、を備えた認証局と、上記認証局が発行した上記証明書を格納する証明書格納手段を備えた証明書リポジトリと、上記認証局が発行した上記ＣＲＬを格納するＣＲＬ格納手段を備えたＣＲＬリポジトリと、上記証明書の有効性を検証する証明書有効性検証手段と、上記ＣＲＬリポジトリから取得した上記ＣＲＬをキャッシュするＣＲＬキャッシュ手段と、上記証明書有効性検証手段が上記証明書の有効性を検証するために構築した検証パスをキャッシュする検証パスキャッシュ手段と、を備えた証明書検証サーバと、電子署名を検証する電子署名検証手段と、上記証明書検証サーバに上記証明書の有効性検証を依頼する証明書有効性検証依頼手段と、を備えたクライアントと、から構成される、認証基盤システムにおいて、上記認証局に、上記ＣＲＬを発行すると同時に、上記証明書検証サーバに「上記ＣＲＬが発行された」旨を通知する、ＣＲＬ発行通知を送信する、ＣＲＬ発行通知送信手段、を設け、上記証明書検証サーバに、上記認証局から上記ＣＲＬ発行通知を受信する、ＣＲＬ発行通知受信手段、を設けたことを特徴とする。

【００２１】

また、本発明は、上記証明書検証サーバの上記ＣＲＬキャッシュ手段は、上記ＣＲＬ発行通知受信手段によって、上記ＣＲＬ発行通知を受信した場合に、上記認証局

が新たに発行した上記ＣＲＬを上記ＣＲＬリポジトリから取得するものであること、を特徴とする。

【００２２】

さらに、本発明は、上記証明書検証サーバに、上記ＣＲＬが新たに発行されたことを発見した場合に、予め登録された、他の証明書検証サーバに対して、「ＣＲＬが発行された」旨を通知する、ＣＲＬ発行通知送信手段、を設けたことを特徴とする。

【００２３】

また、本発明は、上記認証局に、上記証明書発行手段によって上記証明書が発行された場合に、上記証明書検証サーバに「証明書が発行された」旨を通知する証明書発行通知を送信する、証明書発行通知送信手段を設け、前記証明書検証サーバに、上記証明書発行通知を受信する、証明書発行通知受信手段を設け、上記証明書有効性検証手段は、上記証明書発行通知受信手段が上記証明書発行通知を受信した場合に、新たに発行された上記証明書を含むような、上記検証パスを作成するものであって、上記検証パスキャッシュ手段は当該検証パスをキャッシュするものであること、を特徴とする。

【００２４】

さらに、本発明は、上記証明書検証サーバに、上記検証パスを構築した場合に、予め登録された、他の証明書検証サーバに当該検証パスを送信する、検証パス送信手段を設け、上記検証パスキャッシュ手段は、他の証明書検証サーバから上記検証パスを受信した場合に、当該検証パスをキャッシュするものであること、を特徴とする。

【００２５】

さらに、本発明は、上記クライアントは、上記電子署名を検証するために必要な、上記証明書の取得を、上記証明書検証サーバに依頼する、証明書取得依頼手段、を設け、上記証明書検証サーバに、上記クライアントから取得を要求された上記証明書を上記証明書リポジトリから取得し、かつ、上記証明書検証手段によって、当該証明書が有効であると判定された場合に、上記クライアントに当該証明書を送信する、証明書取得手段、を設けたことを特徴とする。

【００２６】

さらに、本発明は、「上記ＣＲＬ発行通知の送信を依頼する」旨のメッセージを作成する手段を上記証明書検証サーバに設け、上記ＣＲＬ発行通知依頼メッセージを受信する手段を上記認証局に設け、さらに、上記認証局の上記ＣＲＬ発行通知送信手段は、当該認証局に対して上記ＣＲＬ発行通知依頼メッセージを送信してきた証明書検証サーバに対して、上記ＣＲＬ発行通知を送信することを特徴とする。

【００２７】

また、本発明は、上記ＣＲＬリポジトリに新たなＣＲＬが格納されたことを発見した場合に、「ＣＲＬが発行された」旨のＣＲＬ発行通知を送信するＣＲＬ発行通知送信手段と、「上記ＣＲＬ発行通知の送信を依頼する」旨のＣＲＬ発行通知依頼メッセージを受信するＣＲＬ発行通知依頼受信手段とを、上記ＣＲＬリポジトリに備えたことを特徴とする。

【００２８】

また、本発明のＣＲＬ発行確認ソフトウェアは、ＣＲＬの発行を監視し、新たなＣＲＬの発行された場合に、ＣＲＬ発行通知を送信する手段を実現するものであり、ＣＲＬ発行通知依頼メッセージを受信する手段を実現し、上記ＣＲＬ発行通知送信手段は、上記ＣＲＬ発行通知を受信した上記ＣＲＬ発行通知依頼メッセージの送信元に送信することを特徴とする。

【００２９】

さらに、本発明の上記証明書検証サーバは、前記ＣＲＬ発行通知依頼作成手段によって作成されたＣＲＬ発行通知依頼メッセージを受信する手段を設けたことを特徴とする。

【００３０】

【発明の実施の形態】

以下、図面を用いて本発明の実施の形態について説明する。なお、これによって本発明が限定されるものではない。

【００３１】

図１は、本発明の実施例である電子署名付き電子文書交換システムの一構成を示した図である。認証局１$_1$から認証局１$_9$までの９個の認証局（以下、まとめて、認証局１、と記述する）と、証明書リポジトリ２と、ＣＲＬリポジトリ３と、証明書検証サーバ４$_1$から証明書検証サーバ４$_n$までのｎ個の証明書検証サーバ（以下、まとめて、証明書検証サーバ４、と記述する）と、上記証明書検証サーバ４に証明書の有効性の検証を依頼する、クライアント端末５$_1$からクライアント端末５$_m$までのｍ個のクライアント端末（以下、まとめて、クライアント端末５、と記述する）と、がネットワーク０を介して接続されている。

【００３２】

上記認証局１は、上記クライアント端末５に証明書５０９を発行し、かつ、当該証明書５０９のコピーを上記証明書リポジトリ２に格納する証明書発行機能１０１と、失効した上記証明書５０９のリストであるＣＲＬ７を発行し、かつ、当該ＣＲＬ７を上記ＣＲＬリポジトリに格納するＣＲＬ発行機能１０２と、上記ＣＲＬ７が発行されたことを通知するＣＲＬ発行通知８を、上記証明書検証サーバ４に対して送信する、ＣＲＬ発行通知機能１０３と、「上記ＣＲＬ発行通知８の送信を依頼する」旨の、ＣＲＬ発行通知依頼メッセージ１０を受信するＣＲＬ発行通知依頼受信機能１０５と、を備えている。

【００３３】

また、認証局１$_1$から認証局１$_9$までの、上記認証局１は、相互認証証明書９を発行しあい、図２に示したよう

な、相互認証の関係がある。

【００３４】

上記証明書リポジトリ２は、上記証明書５０９を保持する、証明書ＤＢ２０１と、上記認証局１から上記証明書５０９を受信し、かつ、当該証明書５０９を上記証明書ＤＢ２０１に格納し、さらには、指定された上記証明書５０９を上記証明書ＤＢ２０１から検索して返信する、証明書ＤＢ管理機能２０２と、を備えている。

【００３５】

上記ＣＲＬリポジトリ３は、上記ＣＲＬ７を保持する、ＣＲＬＤＢ３０１と、上記認証局１から上記ＣＲＬ７を受信し、かつ、当該ＣＲＬを上記ＣＲＬＤＢ３０１に格納し、さらには、指定された上記ＣＲＬ７を上記ＣＲＬＤＢ３０１から検索して返信する、証明書ＤＢ管理機能３０２と、を備えている。

【００３６】

上記証明書検証サーバ４は、

上記ＣＲＬ７をキャッシュしたＣＲＬキャッシュ４０１と、

上記証明書５０９の有効性を検証するために使用する、検証パスをキャッシュした検証パスキャッシュ４０２と、

上記クライアント端末５からの要求を受けて、証明書の有効性を検証する証明書検証機能４０３と、

上記クライアント端末５からの要求を受けて、上記証明書リポジトリ２から上記証明書５０９を取得し、かつ、当該証明書５０９の有効性を上記証明書検証機能４０３によって検証し、さらには、当該証明書５０９が有効であった場合に上記クライアント端末５に返信する、証明書取得機能４０４と、

上記ＣＲＬリポジトリ３から上記ＣＲＬ７を取得し、かつ、当該ＣＲＬ７を上記ＣＲＬキャッシュ４０１に格納する、ＣＲＬ管理機能４０５と、

上記認証局１から上記ＣＲＬ発行通知８を受信し、かつ、上記認証局１から上記ＣＲＬ発行通知８を受け取った場合に、予め登録された、あるいは、上記ＣＲＬ発行通知依頼メッセージ１０を送信することにより当該ＣＲＬ発行通知８の転送を依頼してきた、他の証明書検証サーバ４に当該ＣＲＬ発行通知８を転送する、ＣＲＬ発行通知管理機能４０６と、

上記証明書検証機能４０３が作成した上記検証パスを上記検証パスキャッシュ４０２にキャッシュし、かつ、当該検証パスを予め登録された他の証明書検証サーバ４に対して送信し、さらには、他の証明書検証サーバ４から受信した上記検証パスを上記検証パスキャッシュ４０２にキャッシュする、検証パス管理機能４０７と、

上記認証局１に対して上記ＣＲＬ発行通知８の送信を依頼する、ＣＲＬ発行通知依頼メッセージ１０を作成する、ＣＲＬ発行通知依頼作成機能４１０と、

他の証明書検証サーバ４から上記ＣＲＬ発行通知依頼メッセージ１０を受信する、ＣＲＬ発行通知依頼受信機能４１１と、を備えている。

【００３７】

上記クライアント端末５は、

他のクライアント端末５と電子文書６を交換する、電子文書交換機能５０１と、

上記電子文書６に電子署名を行い、かつ、他のクライアント端末５から受信した上記電子文書６に行われた電子署名を検証する、電子署名機能５０２と、

上記証明書検証サーバ４に上記証明書５０９の有効性の検証を要求し、かつ、上記証明書検証サーバ４から上記証明書５０９の有効性検証の結果を受信する、証明書検証要求機能５０３と、

上記電子文書６に上記証明書５０９ではなく、上記証明書５０９の格納場所を示したＵＲＬが添付されていた場合に、当該ＵＲＬに格納されている上記証明書５０９を取得するために上記証明書検証サーバ４に当該証明書識別情報を送信し、かつ、上記証明書検証サーバ４から当該証明書５０９を受信する、証明書取得依頼機能５０６と、

上記電子署名作成機能５０２が利用する、秘密鍵５０８と、

上記認証局１が発行した、上記証明書５０９と、を備えている。

【００３８】

なお、上記クライアント端末５$_1$の上記証明書５０９$_1$は上記認証局１$_1$から発行されており、上記クライアント端末５$_2$の上記証明書５０９$_2$は上記認証局１$_2$から発行されている。

【００３９】

また、本実施例では、上記証明書検証要求機能５０３と、上記証明書取得依頼機能５０６と、が利用する上記証明書検証サーバ４は、上記証明書検証サーバ４$_1$から上記証明書検証サーバ４$_n$までの上記証明書検証サーバ４のうち、予め定められた、特定の上記証明書検証サーバ４を利用する。

【００４０】

例えば、クライアント端末５$_2$は上記証明書検証サーバ４$_1$を利用する。

【００４１】

なお、図１に示す認証局１、証明書リポジトリ２、ＣＲＬリポジトリ３、証明書検証サーバ４、クライアント端末５、の各装置は、例えば、図９に示すような、ＣＰＵ９１と、メモリ９２と、ハードディスク等の外部記憶装置９３と、ＣＤ－ＲＯＭ等の可搬性を有する記憶媒体９９から情報を読み取る読取装置９４と、ネットワークを介して他装置と通信を行うための通信装置９５と、キーボードやマウス等の入力装置９６と、モニタやプリンタ等の出力装置９７と、これらの各装置間のデータ送受を行うインターフェース９８とを備えた、一般的な電子計

算機において、ＣＰＵ９１がメモリ９２上にロードされた所定のプログラムを実行することにより、実現できる。

【００４２】

すなわち、証明書発行機能１０１、ＣＲＬ発行機能１０２、ＣＲＬ発行通知機能１０３、ＣＲＬ発行通知依頼受信機能１０５、証明書ＤＢ管理機能２０２、ＣＲＬＤＢ管理機能３０２、証明書検証機能４０３、証明書取得機能４０４、ＣＲＬ管理機能４０５、ＣＲＬ発行通知管理機能４０６、検証パス管理機能４０７、ＣＲＬ発行通知依頼作成機能４１０、ＣＲＬ発行通知依頼受信機能４１１、電子文書交換機能５０１、電子署名機能５０２、証明書検証要求機能５０３、証明書取得依頼機能５０４、はＣＰＵ９１が所定のプログラムを実行することによるプロセスとして実現できる。また、証明書ＤＢ２０１、ＣＲＬＤＢ３０１、ＣＲＬキャッシュ４０１、検証パスキャッシュ４０２、は、ＣＰＵ９１がメモリ９２や外部記憶装置６３を利用することにより実現できる。

【００４３】

このような電子計算機上に、上記各装置を実現するための所定のプログラムは、読取装置９４を介して電子計算機が利用可能な記憶媒体９９から導入されてもよいし、あるいは、通信装置９６を介してネットワークまたはネットワークを伝搬する搬送波といった、電子計算機が利用可能な通信媒体を介して他のサーバから導入されてもよい。

【００４４】

導入に際しては、一旦、外部記憶装置９３に格納された後、そこからメモリ９２上にロードされてＣＰＵ９１に実行されてもよいし、あるいは、外部記憶装置９３に格納されることなく、直接メモリ９２上にロードされて、ＣＰＵ９１に実行されてもよい。

【００４５】

次に、図１の電子署名利用システムの動作について、上記証明書検証サーバ４が上記認証局１に対して上記ＣＲＬ発行通知８の送信を依頼する場合の動作について、図面を用いて説明する。

【００４６】

図７は、図１の電子署名利用システムにおいて、上記証明書検証サーバ４が上記認証局１に対して上記ＣＲＬ発行通知８の送信を依頼する場合の、上記証明書検証サーバ４と、上記認証局１と、の動作を示す。

【００４７】

上記証明書検証サーバ４において、上記ＣＲＬ発行通知依頼作成機能４１０が、上記ＣＲＬ発行通知依頼メッセージ１０を作成し（ステップ７１０１）、上記認証局１に送信する（ステップ７１０２）。

【００４８】

図８（ａ）に例示する、ＣＲＬ発行通知依頼メッセージ１０は、「上記ＣＲＬ発行通知８の送信を依頼する」旨

のメッセージと、上記ＣＲＬ発行通知８の送信先となるネットワーク０上のアドレスであるホスト名と、から構成されている。

【００４９】

上記認証局１では、上記ＣＲＬ発行通知依頼受信機能１０５が、上記ＣＲＬ発行通知依頼メッセージ１０を受信する（ステップ７２０１）と、当該ＣＲＬ発行通知依頼メッセージ１０を送信してきた、上記証明書検証サーバ４のホスト名をＣＲＬ発行通知送信先リスト１０４に追加する（ステップ７２０２）。

【００５０】

上記証明書検証サーバ４$_1$から上記証明書検証サーバ４$_2$への上記ＣＲＬ発行通知８の転送を依頼する場合には、まず、上記証明書検証サーバ４$_1$の上記ＣＲＬ発行通知依頼作成機能４１０が上記ＣＲＬ発行通知依頼メッセージ１０を作成し、上記証明書検証サーバ４$_2$に送信する。

【００５１】

上記証明書検証サーバ４$_2$のＣＲＬ発行通知依頼受信機能４１１は、当該ＣＲＬ発行通知依頼メッセージ１０を受信し、送信元である上記証明書検証サーバ４のホスト名をＣＲＬ発行通知転送先リスト４０８に追加する。

【００５２】

上記証明書検証サーバ４が上記認証局１に対して上記ＣＲＬ発行通知８の送信停止を依頼する場合には、図８（ｂ）に例示するような、ＣＲＬ発行通知依頼メッセージ１０を、上記認証局１に送信する。

【００５３】

図８（ｂ）のＣＲＬ発行通知依頼メッセージ１０は、「上記ＣＲＬ発行通知８の送信停止を依頼する」旨のメッセージと、上記ＣＲＬ発行通知８の送信先のホスト名と、から構成されている。

【００５４】

上記認証局１は、図８（ｂ）のＣＲＬ発行通知依頼メッセージ１０を受信したら、記載されている上記証明書検証サーバ４のホスト名をＣＲＬ発行通知転送先リスト４０８から削除する。

【００５５】

上記証明書検証サーバ４が、他の証明書検証サーバ４に上記ＣＲＬ発行通知８の転送を依頼したり、転送停止を依頼したりする場合には、依頼先の証明書検証サーバ４に、上記ＣＲＬ発行通知依頼メッセージ１０を送信する。

【００５６】

次に、図１の電子署名利用システムにおいて、上記ＣＲＬ７が発行された場合の、上記認証局１と、上記ＣＲＬリポジトリ３と、上記証明書検証サーバ４と、の動作について、図面を用いて説明する。

【００５７】

図３は、図１の電子署名利用システムにおいて、上記Ｃ

15

ＲＬ７が発行された場合の、上記認証局１と、上記ＣＲＬリポジトリ３と、上記証明書検証サーバ４と、の動作を示す図である。

【００５８】

まず、上記認証局１の動作について説明する。

【００５９】

上記認証局１は、上記ＣＲＬ発行機能１０２が上記ＣＲＬ７を作成する（ステップ３１０１）と、当該ＣＲＬ発行機能１０２が当該ＣＲＬ７を上記ＣＲＬリポジトリ３に送信する（ステップ３１０２）。

【００６０】

次に、上記ＣＲＬ発行通知機能１０３が、上記ＣＲＬ発行通知８を作成し、予め定められた、あるいは、上記ＣＲＬ発行通知依頼メッセージ１０を送信することにより当該ＣＲＬ発行通知８の送信を依頼してきた、上記証明書検証サーバ４に送信する（ステップ３１０３）。

【００６１】

なお、本実施例では、認証局１は、ＣＲＬ発行通知送信先リスト１０４にホスト名が記載されている、上記証明書検証サーバ４に上記ＣＲＬ発行通知８を送信する。

【００６２】

図６の（ａ）は、上記認証局１が管理しているＣＲＬ発行通知送信先リスト１０４の一例であり、上記証明書検証サーバ４$_1$のホスト名と、上記証明書検証サーバ４$_n$のホスト名と、が記載されている。

【００６３】

したがって、上記認証局１の上記ＣＲＬ発行通知機能１０３は、上記証明書検証サーバ４$_1$と、上記証明書検証サーバ４$_n$と、に上記ＣＲＬ発行通知８を送信する。

【００６４】

次に、上記ＣＲＬリポジトリ３の動作について説明する。

【００６５】

上記ＣＲＬリポジトリ３の上記ＣＲＬＤＢ管理機能３０２は、上記認証局１、あるいは、上記証明書検証サーバ４からのアクセスを待ち受け、上記認証局１から上記ＣＲＬ７を受信する（ステップ３３０１）と、当該ＣＲＬ７を上記ＣＲＬＤＢ３０１格納し（ステップ３３０２）、再び、上記認証局１、あるいは、上記証明書検証サーバ４からのアクセスを待ち受ける。

【００６６】

一方、上記証明書検証サーバ４から、上記ＣＲＬ７を送信するように依頼を受ける（ステップ３３０３）と、上記ＣＲＬＤＢ３０１から当該ＣＲＬ７を検索し（ステップ３３０４）、上記証明書検証サーバ４に当該ＣＲＬ７を送信して（ステップ３３０５）、再び、上記認証局１、あるいは、上記証明書検証サーバ４からのアクセスを待ち受ける。

【００６７】

次に、上記証明書検証サーバ４の動作について説明する。

16

【００６８】

ここでは、上記認証局１から上記ＣＲＬ発行通知８を受信する上記証明書検証サーバ４$_1$の動作によって、上記証明書検証サーバ４の動作を説明する。

【００６９】

まず、上記証明書検証サーバ４$_1$では、上記ＣＲＬ発行通知管理機能４０６が、上記認証局１、あるいは、他の証明書検証サーバ４、から上記ＣＲＬ発行通知８を受信する（ステップ３４０１）と、まず、当該ＣＲＬ発行通知８を既に受信したかどうかを調べ（ステップ３４０２）、当該ＣＲＬ発行通知８を既に受信していた場合には、そのまま処理を終了する。

【００７０】

一方、上記ＣＲＬ発行通知８を初めて受信した場合には、上記ＣＲＬ管理機能４０５が、上記ＣＲＬリポジトリ３にアクセスし（ステップ３４０３）、上記ＣＲＬ７を取得し（ステップ３４０４）、上記ＣＲＬキャッシュ４０１キャッシュする（ステップ３４０５）。

【００７１】

次に、上記ＣＲＬ発行通知管理機能４０６は、予め登録された、あるいは、上記ＣＲＬ発行通知依頼メッセージ１０を送信することにより当該ＣＲＬ発行通知８の転送を依頼してきた、他の証明書検証サーバ４に、上記ＣＲＬ発行通知８を転送する（ステップ３４０６）。

【００７２】

上記証明書検証サーバ４は、ＣＲＬ発行通知転送先リスト４０８というリストを利用して、上記ＣＲＬ発行通知６を転送する、上記証明書検証サーバ４を管理している。

【００７３】

図６の（ｂ）は、上記証明書検証サーバ４$_1$が管理している上記ＣＲＬ発行通知転送先リスト４０８の一例であり、上記証明書検証サーバ４$_2$のホスト名と、上記証明書検証サーバ４$_3$のホスト名と、上記証明書検証サーバ４$_n$のホスト名とが記載されている。

【００７４】

したがって、上記ＣＲＬ発行通知管理機能４０６は、上記ＣＲＬ発行通知６を、上記証明書検証サーバ４$_2$と、上記証明書検証サーバ４$_3$と、上記証明書検証サーバ４$_n$に転送する。

【００７５】

なお、本実施例では、上記証明書検証サーバ４$_1$から上記証明書検証サーバ４$_n$までの各々のホスト名は、上記証明書検証サーバ４$_1$から上記証明書検証サーバ４$_n$までの証明書検証サーバ４が各々に保持している、上記ＣＲＬ発行通知転送先リスト４０８のいずれかに必ず記載されているようにしている。

【００７６】

こうすることにより、どれか一つの上記証明書検証サー

バ４が上記認証局１から上記ＣＲＬ発行通知６を受け取れば、上記証明書検証サーバ４$_1$から上記証明書検証サーバ４$_n$までのすべての証明書検証サーバ４が上記ＣＲＬ発行通知６を受け取ることができる。

【００７７】

また、上記証明書検証サーバ４を新たに追加する場合には、上記証明書検証サーバ４$_1$から上記証明書検証サーバ４$_n$までの証明書検証サーバ４が各々に保持している、上記ＣＲＬ発行通知転送先リスト４０８のいずれかに当該証明書検証サーバ４のホスト名を追加すれば、上記ＣＲＬ発行通知送信先リスト１０４を変更する必要はなくなる。

【００７８】

以上が、上記ＣＲＬ７が発行された場合の、図１の電子署名利用システムの動作である。

【００７９】

次に、図１の電子署名付き電子文書交換システムにおいて、上記クライアント端末５$_1$から、上記クライアント端末５$_2$に、上記電子文書６を送信する場合の動作について、図面を用いて説明する。

【００８０】

なお、本実施例では、上記電子文書６に施された電子署名を検証するための上記証明書５０９は、上記電子文書６に添付される場合と、上記電子文書６に添付されない場合と、の二つの場合があるが、まずは、上記電子文書６に施された電子署名を検証するための上記証明書５０９が、上記電子文書６に添付される場合について説明する。

【００８１】

図４は、図１の電子署名付き電子文書交換システムにおいて、上記電子文書６に施された電子署名を検証するための上記証明書５０９が、上記電子文書６に添付される場合に、上記クライアント端末５$_1$から、上記クライアント端末５$_2$に、上記電子文書６を送信する際の、上記クライアント端末５$_1$と、上記クライアント端末５$_2$と、上記証明書検証サーバ４$_1$と、上記証明書検証サーバ４$_2$と、の動作を示した図である。

【００８２】

まず、上記クライアント端末５$_1$の動作について説明する。

【００８３】

上記クライアント端末５$_1$は、上記電子文書交換機能５０１が、上記クライアント端末５$_2$に送信する、上記電子文書６を作成する（ステップ４５０１）と、上記電子署名機能５０２が、上記秘密鍵５０８$_1$を使用して、当該電子文書６に電子署名を施す（ステップ４５０２）。

【００８４】

次に、上記電子文書交換機能５０１は、電子署名が施された、上記電子文書６を、上記証明書５０９$_1$とともに、上記クライアント端末５$_2$に送信する（ステップ４５０３）。

【００８５】

次に、上記クライアント端末５$_2$の動作について説明する。

【００８６】

上記クライアント端末５$_2$は、上記電子文書６を受信する（ステップ４５１１）と、上記電子文書６とともに送信されてきた上記証明書５０９$_1$の有効性を検証するため、上記証明書有効性確認機能５０３が、上記証明書検証サーバ４$_1$に当該証明書５０９$_1$の有効性検証を依頼し（ステップ４５１２）、上記証明書検証サーバ４$_1$から有効性検証の結果を受信する（ステップ４５１３）。

【００８７】

ここで、上記有効性検証の結果が、上記証明書５０９$_1$は、上記クライアント端末５$_2$にとって有効ではない、というものであった場合、処理を終了する。

【００８８】

一方、上記有効性検証の結果が、上記証明書５０９$_1$は、上記クライアント端末５$_2$にとって有効である、というものであった場合、上記電子署名機能５０３は、上記証明書５０９$_1$から公開鍵を取り出し、上記電子文書６に施されている電子署名を検証する（ステップ４５１５）。ここで、上記電子署名が正しくないと判定された場合には処理を終了する。

【００８９】

一方、上記電子署名が正しいと判定された場合には、上記電子署名６を保存する（ステップ４５１６）。

【００９０】

次に、上記証明書検証サーバ４の動作について説明する。

【００９１】

まず、上記証明書検証サーバ４$_1$は、上記クライアント端末５$_2$から上記証明書５０９$_1$の有効性検証を依頼される（ステップ４４０１）と、上記証明書検証機能４０３が、上記クライアント端末５$_2$から上記クライアント端末５$_1$までの検証パスが、上記検証パスキャッシュ４０２に存在しているかを確認する（ステップ４４０２）。

【００９２】

ここで、上記検証パスキャッシュ４０２に、当該検証パスが存在する場合には、ステップ４４０４に進む。一方、上記検証パスキャッシュ４０２に、当該検証パスが存在しなかった場合には、当該検証パスを構築し（ステップ４４０３）、ステップ４４０４に進む。

【００９３】

ステップ４４０４では、上記証明書検証４０３は、上記ＣＲＬキャッシュ４０１から上記ＣＲＬ７を取り出し、上記検証パスが有効か否かを判定する。次に、判定結果を上記クライアント端末５$_2$に送信する（ステップ４４０５）。

【００９４】
ここで、上記検証パスが、ステップ４４０３で新たに構築されたものでない場合には、処理を終了する。一方、上記検証パスが、ステップ４４０３で新たに構築されたものであった場合には、検証パス送信先リスト４０９にホスト名が記載されている、上記証明書検証サーバ４に当該検証パスを送信し（ステップ４４０７）、処理を終了する。

【００９５】
上記検証パス送信先リスト４０９は、新たに構築した上記検証パスを送信する上記証明書検証サーバ４のホスト名を記載したリストであり、本実施例では、上記ＣＲＬ発行通知転送先リスト４０８を上記検証パス送信先リスト４０９にも利用している。

【００９６】
したがって、ステップ４４０７では、上記検証パスは、上記証明書検証サーバ４_2と、上記証明書検証サーバ４_3と、上記証明書検証サーバ４_nと、に送信される。

【００９７】
なお、本実施例では、上記ＣＲＬ発行通知転送先リスト４０８と、上記検証パス送信先リスト４０９と、に同じリストを使用しているが、本発明はそれに限定されるものではなく、個々に異なるリストを利用しても良い。

【００９８】
一方、上記証明書検証サーバ４_2や、上記証明書検証サーバ４_3や、上記証明書検証サーバ４_nは、上記証明書検証サーバ４_1から上記検証パスを受信する（ステップ４４１１）と、上記検証パス管理機能４０７は当該検証パスが上記検証パスキャッシュ４０２にキャッシュされているかどうかを確認する（ステップ４４１２）。

【００９９】
ここで、上記検証パスキャッシュ４０２に上記検証パスがキャッシュされていれば、何もせず、処理を終了する。一方、上記検証パスキャッシュ４０２に上記検証パスがキャッシュされていなければ、当該検証パスを上記検証パスキャッシュ４０２にキャッシュし（ステップ４４１３）、検証パス送信先リスト４０９にホスト名が記載されている、上記証明書検証サーバ４に当該検証パスを送信し（ステップ４４１４）、処理を終了する。

【０１００】
なお、本実施例では、上記証明書検証サーバ４の上記検証パス管理機能４０７は、検証パスを送受したり、キャッシュしたりするようにしているが、本発明はそれに限定されるものではなく、上記検証パスを一意に識別できるような検証パス情報を送受したり、キャッシュしたりし、必要なときに当該検証パス情報から対応する検証パスを構成するようにしてもよい。

【０１０１】
以上が、上記電子文書６に施された電子署名を検証するための上記証明書５０９が上記電子文書６に添付される場合の、上記クライアント端末５_1から上記クライアント端末５_2に上記電子文書６を送信する際の、図１の電子署名付き電子文書交換システムの動作である。

【０１０２】
次に、上記電子文書６に施された電子署名を検証するための上記証明書５０９が上記電子文書６に添付されない場合の、上記クライアント端末５_1から上記クライアント端末５_2に上記電子文書６を送信する際の、図１の電子署名付き電子文書交換システムの動作について、図面を用いて説明する。

【０１０３】
図５は、図１の電子署名付き電子文書交換システムにおいて、上記電子文書６に施された電子署名を検証するための上記証明書５０９が、上記電子文書６に添付されない場合に、上記クライアント端末５_1から上記クライアント端末５_2に上記電子文書６を送信する際の、上記クライアント端末５_1と、上記クライアント端末５_2と、上記証明書検証サーバ４と、上記証明書リポジトリ２と、の動作を示した図である。

【０１０４】
まず、上記クライアント端末５_1の動作について説明する。

【０１０５】
上記クライアント端末５_1は、上記電子文書交換機能５０１が、上記クライアント端末５_2に送信する、上記電子文書６を作成する（ステップ５５０１）と、上記電子署名機能５０２が、上記秘密鍵５０８_1を使用して、当該電子文書６に電子署名を施す（ステップ５５０２）。

【０１０６】
次に、上記電子文書交換機能５０１は、電子署名が施された、上記電子文書６を、上記証明書５０９_1の格納場所を示したＵＲＬとともに、上記クライアント端末５_2に送信する（ステップ５５０３）。

【０１０７】
なお、本実施例では、上記電子文書６とともに、上記証明書５０９の格納場所を示したＵＲＬを送信するようにしているが、本発明はこれに限定されるものではなく、上記証明書５０９に記載されている情報の一部を送信するようにしてもよい。

【０１０８】
次に、上記クライアント端末５_2の動作について説明する。

【０１０９】
上記クライアント端末５_2は、上記電子文書６を受信する（ステップ５５１１）と、上記証明書取得依頼機能５０４が、上記電子文書６とともに送信されてきた上記ＵＲＬに対応する上記証明書５０９_1を上記証明書検証サーバ４_1に取得するように依頼し（ステップ５５１２）、上記証明書検証サーバ４_1から依頼結果を受信する（ステップ５５１３）。

【０１１０】
ここで、上記依頼結果に上記証明書５０９$_1$が含まれていなかった場合、すなわち、上記ＵＲＬが示す上記証明書５０９$_1$が上記クライアント端末５$_2$にとって有効なものでない、と上記証明書検証サーバ４$_1$が判断した場合には、処理を終了する。一方、上記依頼結果に上記証明書５０９$_1$が含まれていた場合、上記電子署名機能５０３は、上記証明書５０９$_1$から公開鍵を取り出し、上記電子文書６に施されている電子署名を検証する（ステップ５５１５）。ここで、上記電子署名が正しくないと判定された場合には、処理を終了する。一方、上記電子署名が正しいと判定された場合には、上記電子署名６を保存し（ステップ５５１６）、処理を終了する。

【０１１１】
次に、上記証明書検証サーバ４の動作について説明する。

【０１１２】
上記証明書検証サーバ４$_1$の上記証明書取得機能４０４は、上記クライアント端末５$_2$から、上記証明書５０９$_1$を取得するように依頼を受けると（ステップ５４０１）、上記クライアント端末５$_2$から送信された上記ＵＲＬを用いて、上記証明書リポジトリ２にアクセスし（ステップ５４０２）、上記証明書５０９$_1$を取得する（ステップ５４０３）。

【０１１３】
次に、上記証明書検証機能４０３によって、上記証明書５０９$_1$が、上記クライアント端末５$_2$にとって、有効な証明書であるか否かを判定する（ステップ５４０４）。

【０１１４】
ここで、上記証明書検証機能４０３の動作については、図４のステップ４４０２からステップ４４０９までの動作と同じであり、説明を省略する。

【０１１５】
上記判定によって、上記証明書５０９$_1$が、上記クライアント端末５$_2$にとって、有効な証明書である、と判定された場合、当該証明書５０９$_1$を含む依頼結果を作成し（ステップ５４０５）、上記クライアント端末５$_2$に送信する（ステップ５４０７）。一方、上記証明書５０９$_1$が、上記クライアント端末５$_2$にとって、有効な証明書でない、と判定された場合には、「有効でない」旨を示す依頼結果を作成し（ステップ５４０６）として上記クライアント端末５$_2$に送信する（ステップ５４０７）。

【０１１６】
次に、上記証明書リポジトリ２の動作について説明する。

【０１１７】
上記証明書リポジトリ２の上記証明書ＤＢ管理機能２０２は、上記証明書検証サーバ４$_1$から、上記証明書５０９$_1$を送信するように依頼を受ける（ステップ５２０１）と、上記証明書ＤＢ２０１から当該証明書５０９$_1$を検索し（ステップ５２０２）、上記証明書検証サーバ４に当該証明書５０９$_1$を送信する（ステップ５２０３）。

【０１１８】
以上が、上記電子文書６に施された電子署名を検証するための上記証明書５０９が上記電子文書６に添付されない場合の、上記クライアント端末５$_1$から上記クライアント端末５$_2$に上記電子文書６を送信する際の、図１の電子署名付き電子文書交換システムの動作である。

【０１１９】
このように、本実施例の電子署名付き電子文書交換システムでは、上記認証局１が上記ＣＲＬ７を発行する際に、上記ＣＲＬ発行通知８を、上記ＣＲＬ発行通知送信先リスト１０４にホスト名が記載された、上記証明書検証サーバ４に送信することで、上記ＣＲＬ７を発行したことを上記証明書検証サーバ４に通知し、かつ、上記ＣＲＬ発行通知８を受信した上記証明書検証サーバ４は、上記ＣＲＬリポジトリ３から上記ＣＲＬ７を取得して、キャッシュするようにしている。

【０１２０】
このため、上記認証局１が上記ＣＲＬ７を緊急に発行したような場合でも、上記証明書検証サーバ４がキャッシュしているＣＲＬは最新のものであるため、上記証明書５０９の有効性検証結果の精度を保証することができる。

【０１２１】
また、本実施例の電子署名付き電子文書交換システムでは、上記ＣＲＬ発行通知８を受信した上記証明書検証サーバ４は、上記ＣＲＬ発行通知転送先リスト４０８にホスト名が記載されている、他の証明書検証サーバ４に、当該ＣＲＬ発行通知８を転送するようにしている。

【０１２２】
このため、新しく証明書検証サーバ４を追加するような場合でも、上記証明書検証サーバ４の上記ＣＲＬ発行通知転送先リスト４０８に、新たな証明書検証サーバ４のホスト名を記載するだけで、上記ＣＲＬ発行通知８を受信することができるようになり、上記認証局１側の設定を変更する必要はない。

【０１２３】
また、本実施例の電子署名付き電子文書交換システムでは、上記証明書検証サーバ４が、他の証明書検証サーバ４から上記検証パスを受信した場合に、当該検証パスをキャッシュし、かつ、上記証明書検証サーバ４が新たに検証パスを構築した場合には、上記検証パス送信先リスト４０９にホスト名が記載されている、他の証明書検証サーバ４に、当該新たな検証パスを送信するようにしている。

【０１２４】

このため、複数の上記証明書検証サーバ４の間で検証パスを共有することができるため、上記証明書リポジトリ２や上記ＣＲＬリポジトリ３へのアクセスが集中したり、ネットワークの負荷が増大することを防ぐことができる。

【０１２５】

さらに、本実施例の電子署名付き電子文書交換システムでは、上記クライアント端末５が、上記証明書５０９の格納場所を示したＵＲＬを受信した場合に、上記証明書リポジトリ２にアクセスするのではなく、上記証明書検証サーバ４に上記証明書５０９の取得を依頼し、かつ、上記証明書検証サーバ４は、上記証明書リポジトリ２から取得した上記証明書５０９が、上記クライアント端末５にとって有効な証明書であった場合にのみ、上記証明書５０９を上記クライアント端末５に返信するようにしている。

【０１２６】

このため、上記クライアント端末５には、上記証明書リポジトリ２にアクセスする機能を実装する必要がない。

【０１２７】

なお、本実施例では、上記ＣＲＬ発行通知８には、「ＣＲＬが発行された旨」の通知のみが記載されているが、本発明はそれに限定されるものではない。

【０１２８】

例えば、上記ＣＲＬ発行通知８には、新たに発行された上記ＣＲＬ７自身が含まれていたり、あるいは、以前に発行されたＣＲＬ７と、新たに発行されたＣＲＬ７との、差分情報が含まれていたりしてもよい。さらには、新たに失効された証明書５０９の識別情報の一覧が含まれていてもよい。

【０１２９】

上記ＣＲＬ発行通知８に、新たに発行された上記ＣＲＬ７自身や、以前に発行されたＣＲＬ７と新たに発行されたＣＲＬ７との差分情報や、新たに失効された証明書５０９の識別情報の一覧を含めることにより、当該ＣＲＬ発行通知８を受信した上記証明書検証サーバ４は、上記ＣＲＬリポジトリ３にアクセスして新たに発行されたＣＲＬ７を取得する処理を省くことができる。

【０１３０】

また、本実施例では、上記ＣＲＬ発行通知８の送信や、上記ＣＲＬ発行通知依頼メッセージ１０の受信は、上記認証局１が行うようにしているが、本発明はそれに限定されるものではない。例えば、上記ＣＲＬ発行通知８の送信や、上記ＣＲＬ発行通知依頼メッセージ１０の受信を上記ＣＲＬリポジトリ３が行うようにしてもよい。

【０１３１】

あるいは、ＣＲＬリポジトリ３に、上記ＣＲＬ７の発行を監視し、新たなＣＲＬ７が発行されたことを確認した場合に上記ＣＲＬ発行通知８を送信する機能を実現するＣＲＬ発行確認ソフトウェアを導入し、さらに当該ＣＲＬ発行確認ソフトウェアは上記ＣＲＬ発行通知依頼受信機能を実現し、上記ＣＲＬ発行通知送信機能は、受信した上記ＣＲＬ発行通知依頼メッセージの送信元に、上記ＣＲＬ発行通知を送信するようにしてもよい。

【０１３２】

上記ＣＲＬ発行確認ソフトウェアを利用することで、上記ＣＲＬ発行通知送信機能を持たない上記認証局１や上記ＣＲＬリポジトリ３をも利用することが可能になる。さらに、上記ＣＲＬ発行通知依頼受信機能が上記ＣＲＬ発行通知の送信先を管理すれば、上記ＣＲＬリポジトリの運営者と上記証明書検証サーバの運営者とが異なっても上記証明書検証サーバの数を柔軟に変更することができる。

【０１３３】

本実施例によれば、上記ＣＲＬ発行通知は上記認証局が上記ＣＲＬを発行した時に当該認証局から上記証明書検証サーバに対して行われるだけであるので、一定時間毎に上記ＣＲＬが発行されているかどうかを確認する必要がなく、ネットワーク０にかかる負荷が小さくて済む。

【０１３４】

また、上記ＣＲＬ発行通知８は上記認証局１によって行われるため、上記ＣＲＬリポジトリ３と、上記証明書検証サーバ４の運営者が異なる場合でも、高い精度の証明書有効性検証を行うことができる。

【０１３５】

さらに、上記証明書検証サーバ４は、上記ＣＲＬ発行通知依頼メッセージ１０を送信することにより上記ＣＲＬ発行通知８の送信を依頼することができるため、上記ＣＲＬリポジトリ３の運営者と上記証明書検証サーバ４の運営者とが異なっても上記証明書検証サーバ４の数を柔軟に変更することができる。

【０１３６】

さらに、上記証明書検証サーバが新たなＣＲＬが発行されたことを発見した場合、当該証明書検証サーバが他の証明書検証サーバに新たな上記ＣＲＬが発行されたことを通知する。

【０１３７】

送信する上記証明書検証サーバを変更したい場合には、当該証明書検証サーバの設定を変更すればよいため、上記ＣＲＬリポジトリの運営者と上記証明書検証サーバの運営者とが異なっても上記証明書検証サーバの数を柔軟に変更することができる。

【０１３８】

さらに、上記証明書検証サーバが、検証パスを新たに構築した場合、当該検証パスを他の証明書検証サーバにも転送し、検証パスを共有するため、特定の上記ＣＲＬリポジトリや上記証明書リポジトリへのアクセスの集中や、ネットワーク負荷を抑えることができる。

【０１３９】

また、上記証明書を別途入手する方法を利用した場合に

25

も、上記クライアントは、上記証明書リポジトリにアクセスして上記証明書を取得するのではなく、上記証明書検証サーバに、上記証明書を取得し、かつ、当該証明書の有効性を検証するように依頼するため、クライアントに、上記証明書リポジトリにアクセスして上記証明書を取得する機能を実装する必要がない。

【０１４０】

【発明の効果】

したがって、本発明によれば、上記証明書の有効性検証を高い精度と少ない負荷で確実に行なうことができる。

【図面の簡単な説明】

【図１】本発明の一実施形態が適用された、電子署名付き電子文書交換システムのシステム構成を示す図である。

【図２】図１の電子署名付き電子文書交換システムにおいて、認証局１間の相互認証の関係を示す図である。

【図３】図１の電子署名付き電子文書交換システムにおいて、ＣＲＬ７が発行された場合の動作を示す図である。

【図４】図１の電子署名付き電子文書交換システムにおいて、証明書５０９が電子文書とともに送付される場合に、クライアント端末５が電子文書６を送受する際の動作を示す図である。

【図５】図１の電子署名付き電子文書交換システムにおいて、証明書５０９が電子文書とともには送付されない場合に、クライアント端末５が電子文書６を送受する際

26

の動作を示す図である。

【図６】ＣＲＬ発行通知送信先リスト１０４と、ＣＲＬ発行通知転送先リスト４０８の一例を示す図である。

【図７】図１の電子署名付き電子文書交換システムにおいて、証明書検証サーバ４が認証局１に対してＣＲＬ発行通知８の送信を依頼する場合の動作を示す図である。

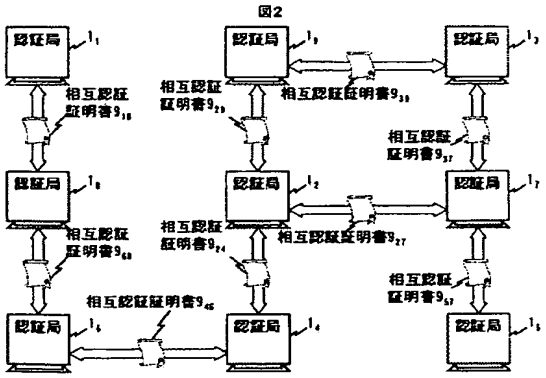
【図８】ＣＲＬ発行通知依頼メッセージ１０の一例を示す図である。

【図９】図１に示す認証局１、証明書リポジトリ２、ＣＲＬリポジトリ３、証明書検証サーバ４、クライアント端末５の各々のハードウエア構成例を示す図である。

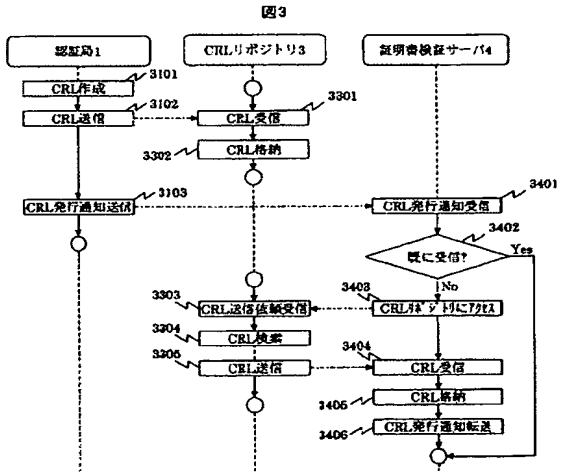
【符号の説明】

０・・・ネットワーク、１、1_1～1_9・・・認証局、２・・・証明書リポジトリ、３・・・ＣＲＬリポジトリ、４、4_1～4_n・・・証明書検証サーバ、５、5_1～5_m・・・クライアント端末、６・・・電子文書、７・・・ＣＲＬ、８・・・ＣＲＬ発行通知、９・・・相互認証証明書、１０・・・ＣＲＬ発行通知依頼メッセージ、９１・・・ＣＰＵ、９２・・・メモリ、９３・・・外部記憶装置、９４・・・読取装置、９５・・・通信装置、９６・・・入力装置、９７・・・出力装置、９８・・・インターフェース、９９・・・記憶媒体、１０４・・・ＣＲＬ発行通知送信先リスト、４０８・・・ＣＲＬ発行通知転送先リスト、４０９・・・検証パス送信先リスト、５０８、508_1～508_m・・・秘密鍵、５０９、509_1～509_m・・・証明書。

【図２】

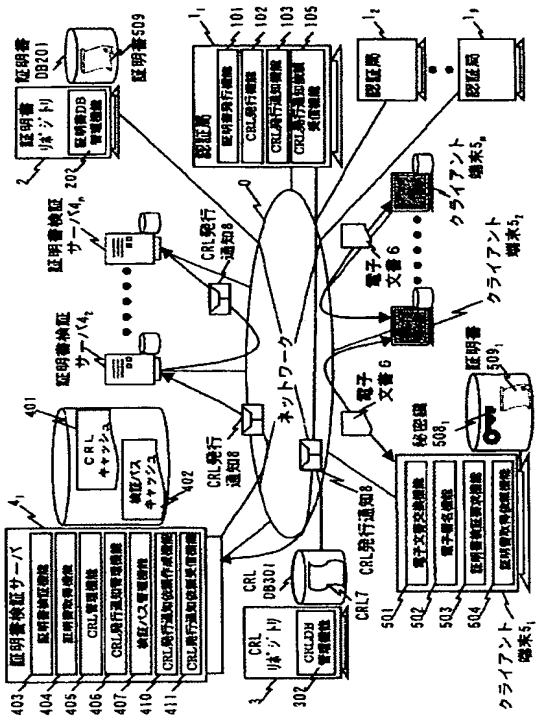


【図３】



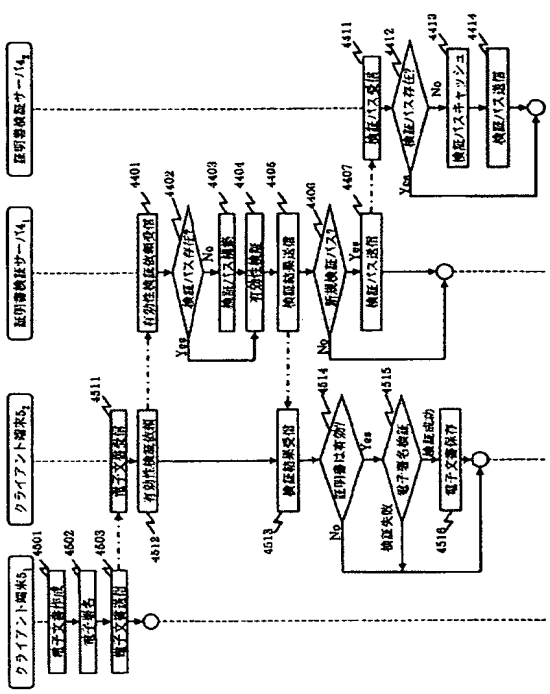
【図１】

図1



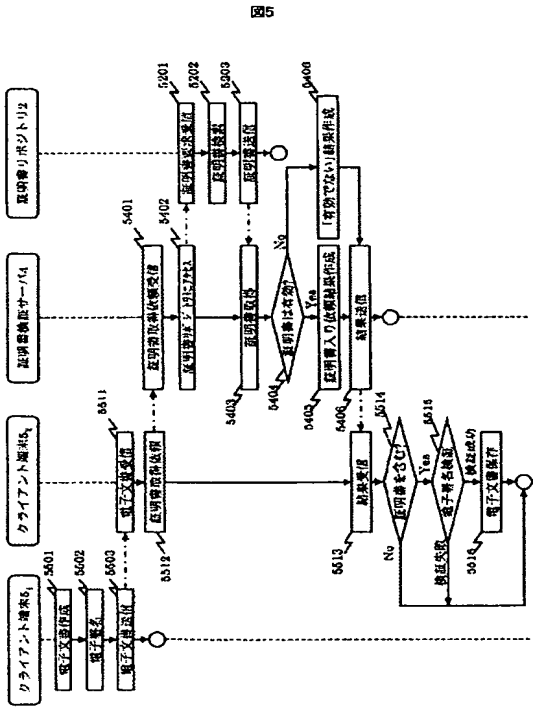
【図４】

図4



【図５】

図5



【図６】

図6

(a) CRL発行通知送信先リスト104

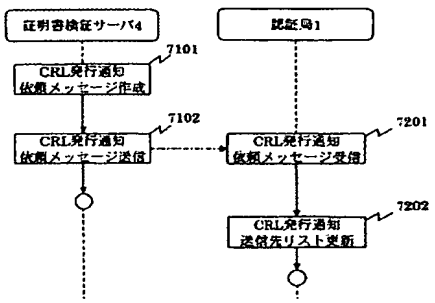
証明書検証サーバ4_1のホスト名	cvs1.va.co.jp
証明書検証サーバ4_nのホスト名	cvs1.certvalidation.com

(b) CRL発行通知転送先リスト408

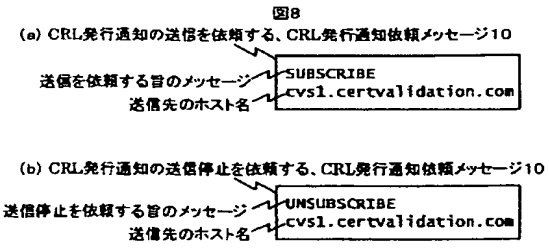
証明書検証サーバ4_2のホスト名	cvs.cvs.org
証明書検証サーバ4_3のホスト名	cvs.certvalidation.co.jp
証明書検証サーバ4_nのホスト名	cvs1.certvalidation.com

【図７】

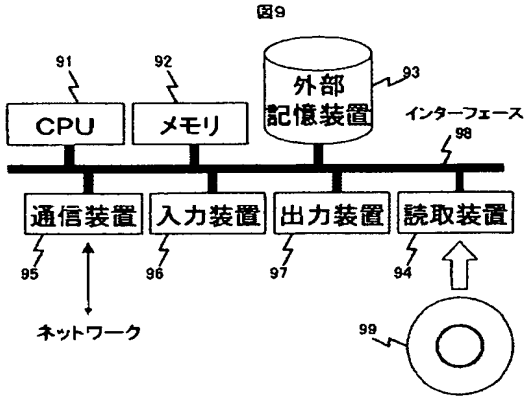
図7



【図８】



【図９】



フロントページの続き

(72)発明者　熊谷　洋子
神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内
(72)発明者　羽根　慎吾
神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内
(72)発明者　長野　裕美
東京都江東区新砂一丁目６番２７号　株式会社日立製作所公共システム事業部内

Ｆターム(参考) 5J104 AA16　EA05　MA01